IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management

IPv6 zone-based firewalls support the Protection of Distributed Denial of Service Attacks and the Firewall Resource Management features.

The Protection Against Distributed Denial of Service Attacks feature provides protection from Denial of Service (DoS) attacks at the global level (for all firewall sessions) and at the VPN routing and forwarding (VRF) level. With the Protection Against Distributed Denial of Service Attacks feature, you can configure the aggressive aging of firewall sessions, event rate monitoring of firewall sessions, half-opened connections limit, and global TCP synchronization (SYN) cookie protection to prevent distributed DoS attacks.

The Firewall Resource Management feature limits the number of VPN Routing and Forwarding (VRF) and global firewall sessions that are configured on a device.

This module describes how to configure the Protection of Distributed Denial of Service Attacks and the Firewall Resource Management features.

- Restrictions for IPv6 Firewall Support for Protection Against Distributed Denial of Service Attacks and Resource Management, on page 2
- Information About IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management, on page 2
- How to Configure IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management, on page 6
- Configuration Examples for IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management, on page 30
- Additional References for IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management , on page 33
- Feature Information for IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management, on page 34

Restrictions for IPv6 Firewall Support for Protection Against Distributed Denial of Service Attacks and Resource Management

The following restriction applies to the Firewall Resource Management feature:

- After you configure the global-level or the virtual routing and forwarding (VRF)-level session limit and reconfigure the session limit, if the global-level or the VRF-level session limit is below the initially configured session count, no new session is added; however, no current session is dropped.

Information About IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management

Aggressive Aging of Firewall Sessions

The Aggressive Aging feature provides the firewall the capability of aggressively aging out sessions to make room for new sessions, thereby protecting the firewall session database from filling. The firewall protects its resources by removing idle sessions. The Aggressive Aging feature allows firewall sessions to exist for a shorter period of time defined by a timer called aging-out time.

The Aggressive Aging feature includes thresholds to define the start and end of the aggressive aging period—high and low watermarks. The aggressive aging period starts when the session table crosses the high watermark and ends when it falls below the low watermark. During the aggressive aging period, sessions will exist for a shorter period of time that you have configured by using the aging-out time. If an attacker initiates sessions at a rate that is faster than the rate at which the firewall terminates sessions, all resources that are allocated for creating sessions are used and all new connections are rejected. To prevent such attacks, you can configure the Aggressive Aging feature to aggressively age out sessions. This feature is disabled by default.

You can configure aggressive aging for half-opened sessions and total sessions at the box level (box refers to the entire firewall session table) and the virtual routing and forwarding (VRF) level. If you have configured this feature for total sessions, all sessions that consume firewall session resources are taken into account. Total sessions comprise established sessions, half-opened sessions, and sessions in the imprecise session database. (A TCP session that has not yet reached the established state is called a half-opened session.)

A firewall has two session databases: the session database and the imprecise session database. The session database contains sessions with 5-tuple (the source IP address, the destination IP address, the source port, the destination port, and the protocol). A tuple is an ordered list of elements. The imprecise session database contains sessions with fewer than 5-tuple (missing IP addresses, port numbers, and so on). In the case of aggressive aging for half-opened sessions, only half-opened sessions are considered.

You can configure an aggressive aging-out time for Internet Control Message Protocol (ICMP), TCP, and UDP firewall sessions. The aging-out time is set by default to the idle time.

Event Rate Monitoring Feature

The Event Rate Monitoring feature monitors the rate of predefined events in a zone. The Event Rate Monitoring feature includes basic threat detection, which is the ability of a security device to detect possible threats, anomalies, and attacks to resources inside the firewall and to take action against them. You can configure a basic threat detection rate for events. When the incoming rate of a certain type of event exceeds the configured threat detection rate, event rate monitoring considers this event as a threat and takes action to stop the threat. Threat detection inspects events only on the ingress zone (if the Event Rate Monitoring feature is enabled on the ingress zone).

The network administrator is informed about the potential threats via an alert message (syslog or high-speed logger [HSL]) and can take actions such as detecting the attack vector, detecting the zone from which the attack is coming, or configuring devices in the network to block certain behaviors or traffic.

The Event Rate Monitoring feature monitors the following types of events:

- Firewall drops due to basic firewall checks failure—This can include zone or zone-pair check failures, or firewall policies configured with the drop action, and so on.
- Firewall drops due to Layer 4 inspection failure—This can include TCP inspections that have failed because the first TCP packet is not a synchronization (SYN) packet.
- TCP SYN cookie attack—This can include counting the number of SYN packets that are dropped and the number of SYN cookies that are sent as a spoofing attack.

The Event Rate Monitoring feature monitors the average rate and the burst rate of different events. Each event type has a rate object that is controlled by an associated rate that has a configurable parameter set (the average threshold, the burst threshold, and a time period). The time period is divided into time slots; each time slot is 1/30th of the time period.

The average rate is calculated for every event type. Each rate object holds 30 completed sampling values plus one value to hold the current ongoing sampling period. The current sampling value replaces the oldest calculated value and the average is recalculated. The average rate is calculated during every time period. If the average rate exceeds the average threshold, the Event Rate Monitoring feature will consider this as a possible threat, update the statistics, and inform the network administrator.

The burst rate is implemented by using the token bucket algorithm. For each time slot, the token bucket is filled with tokens. For each event that occurs (of a specific event type), a token is removed from the bucket. An empty bucket means that the burst threshold is reached, and the administrator receives an alarm through the syslog or HSL. You can view the threat detection statistics and learn about possible threats to various events in the zone from the output of the **show policy-firewall stats zone** command.

You must first enable basic threat detection by using the **threat-detection basic-threat** command. Once basic threat detection is configured, you can configure the threat detection rate. To configure the threat detection rate, use the **threat-detection rate** command.

The following table describes the basic threat detection default settings that are applicable if the Event Rate Monitoring feature is enabled.

Table 1: Basic Threat Detection Default Settings

Packet Drop Reason	Threat Detection Settings
Basic firewall drops	average-rate 400 packets per second (pps) burst-rate 1600 pps rate-interval 600 seconds
Inspection-based firewall drops	average-rate 400 pps burst-rate 1600 pps rate-interval 600 seconds
SYN attack firewall drops	average-rate 100 pps burst-rate 200 pps rate-interval 600 seconds

Half-Opened Connections Limit

The firewall session table supports the limiting of half-opened firewall connections. Limiting the number of half-opened sessions will defend the firewall against attacks that might fill the firewall session table at the per-box level or at the virtual routing and forwarding (VRF) level with half-opened sessions and prevent sessions from being established. The half-opened connection limit can be configured for Layer 4 protocols, Internet Control Message Protocol (ICMP), TCP, and UDP. The limit set to the number of UDP half-opened sessions will not affect the TCP or ICMP half-opened sessions. When the configured half-opened session limit is exceeded, all new sessions are rejected and a log message is generated, either in syslog or in the high-speed logger (HSL).

The following sessions are considered as half-opened sessions:

- TCP sessions that have not completed the three-way handshake.
- UDP sessions that have only one packet detected in the UDP flow.
- ICMP sessions that do not receive a reply to the ICMP echo request or the ICMP time-stamp request.

TCP SYN-Flood Attacks

You can configure the global TCP SYN-flood limit to limit SYN flood attacks. TCP SYN-flooding attacks are a type of denial of service (DoS) attack. When the configured TCP SYN-flood limit is reached, the firewall verifies the source of sessions before creating more sessions. Usually, TCP SYN packets are sent to a targeted end host or a range of subnet addresses behind the firewall. These TCP SYN packets have spoofed source IP addresses. A spoofing attack is when a person or program tries to use false data to gain access to resources in a network. TCP SYN flooding can take up all resources on a firewall or an end host, thereby causing denial of service to legitimate traffic. You can configure TCP SYN-flood protection at the VRF level and the zone level.

SYN flood attacks are divided into two types:

- Host flood—SYN flood packets are sent to a single host intending to utilize all resources on that host.

- Firewall session table flood—SYN flood packets are sent to a range of addresses behind the firewall, with the intention of exhausting the session table resources on the firewall, thereby denying resources to the legitimate traffic going through the firewall.

Firewall Resource Management

Resource Management limits the level of usage of shared resources on a device. Shared resources on a device include:

- Bandwidth
- Connection states
- Memory usage (per table)
- Number of sessions or calls
- Packets per second
- Ternary content addressable memory (TCAM) entries

The Firewall Resource Management feature extends the zone-based firewall resource management from the class level to the VRF level and the global level. Class-level resource management provides resource protection for firewall sessions at a class level. For example, parameters such as the maximum session limit, the session rate limit, and the incomplete session limit protect firewall resources (for example, chunk memory) and keep these resources from being used up by a single class.

When virtual routing and forwarding (VRF) instances share the same policy, a firewall session setup request from one VRF instance can make the total session count reach the maximum limit. When one VRF consumes the maximum amount of resources on a device, it becomes difficult for other VRF instances to share device resources. To limit the number of VRF firewall sessions, you can use the Firewall Resource Management feature.

At the global level, the Firewall Resource Management feature helps limit the usage of resources at the global routing domain by firewall sessions.

Firewall Sessions

Session Definition

At the virtual routing and forwarding (VRF) level, the Firewall Resource Management feature tracks the firewall session count for each VRF instance. At the global level, the firewall resource management tracks the total firewall session count at the global routing domain and not at the device level. In both the VRF and global levels, session count is the sum of opened sessions, half-opened sessions, and sessions in the imprecise firewall session database. A TCP session that has not yet reached the established state is called a half-opened session.

A firewall has two session databases: the session database and the imprecise session database. The session database contains sessions with 5-tuple (source IP address, destination IP address, source port, destination port, and protocol). A tuple is an ordered list of elements. The imprecise session database contains sessions with fewer than 5-tuple (missing IP addresses, port numbers, and so on).

The following rules apply to the configuration of a session limit:

- The class-level session limit can exceed the global limit.
- The class-level session limit can exceed its associated VRF session maximum.
- The sum of the VRF limit, including the global context, can be greater than the hardcoded session limit.

Session Rate

The session rate is the rate at which sessions are established at any given time interval. You can define maximum and minimum session rate limits. When the session rate exceeds the maximum specified rate, the firewall starts rejecting new session setup requests.

From the resource management perspective, setting the maximum and minimum session rate limit helps protect Cisco Packet Processor from being overwhelmed when numerous firewall session setup requests are received.

Incomplete or Half-Opened Sessions

Incomplete sessions are half-opened sessions. Any resource used by an incomplete session is counted, and any growth in the number of incomplete sessions is limited by setting the maximum session limit.

Firewall Resource Management Sessions

The following rules apply to firewall resource management sessions:

- By default, the session limit for opened and half-opened sessions is unlimited.
- Opened or half-opened sessions are limited by parameters and counted separately.
- Opened or half-opened session count includes Internet Control Message Protocol (ICMP), TCP, or UDP sessions.
- You can limit the number and rate of opened sessions.
- You can only limit the number of half-opened sessions.

How to Configure IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management

Configuring an IPv6 Firewall

The steps to configure an IPv4 firewall and an IPv6 firewall are the same. To configure an IPv6 firewall, you must configure the class map in such a way that only an IPv6 address family is matched.

The **match protocol** command applies to both IPv4 and IPv6 traffic and can be included in either an IPv4 policy or an IPv6 policy.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf-definition** *vrf-name* **Example:** `Device(config)# vrf-definition VRF1`	Configures a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode.
Step 4	**address-family ipv6** **Example:** `Device(config-vrf)# address-family ipv6`	Enters VRF address family configuration mode and configures sessions that carry standard IPv6 address prefixes.
Step 5	**exit-address-family** **Example:**	Exits VRF address family configuration mode and enters VRF configuration mode.

	Command or Action	Purpose
	`Device(config-vrf-af)# exit-address-family`	
Step 6	**exit** **Example:** `Device(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 7	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect ipv6-param-map`	Enables a global inspect-type parameter map for the firewall to connect thresholds, timeouts, and other parameters that pertain to the inspect action, and enters parameter-map type inspect configuration mode.
Step 8	**sessions maximum** *sessions* **Example:** `Device(config-profile)# sessions maximum 10000`	Sets the maximum number of allowed sessions that can exist on a zone pair.
Step 9	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 10	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* **Example:** `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	Establishes a port to application mapping (PAM) by using the IPv6 access control list (ACL).
Step 12	**ipv6 access-list** *access-list-name* **Example:** `Device(config)# ipv6 access-list ipv6-acl`	Defines an IPv6 access list and enters IPv6 access list configuration mode.
Step 13	**permit ipv6 any any** **Example:** `Device(config-ipv6-acl)# permit ipv6 any any`	Sets permit conditions for an IPv6 access list.
Step 14	**exit** **Example:** `Device(config-ipv6-acl)# exit`	Exits IPv6 access list configuration mode and enters global configuration mode.
Step 15	**class-map type inspect match-all** *class-map-name* **Example:** `Device(config)# class-map type inspect match-all ipv6-class`	Creates an application-specific inspect type class map and enters QoS class-map configuration mode.

	Command or Action	Purpose
Step 16	**match access-group name** *access-group-name* **Example:** `Device(config-cmap)# match access-group name ipv6-acl`	Configures the match criteria for a class map on the basis of the specified ACL.
Step 17	**match protocol** *protocol-name* **Example:** `Device(config-cmap)# match protocol tcp`	Configures a match criterion for a class map on the basis of the specified protocol.
Step 18	**exit** **Example:** `Device(config-cmap)# exit`	Exits QoS class-map configuration mode and enters global configuration mode.
Step 19	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect ipv6-policy`	Creates a protocol-specific inspect type policy map and enters QoS policy-map configuration mode.
Step 20	**class type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect ipv6-class`	Specifies the traffic class on which an action is to be performed and enters QoS policy-map class configuration mode.
Step 21	**inspect** [*parameter-map-name*] **Example:** `Device(config-pmap-c)# inspect ipv6-param-map`	Enables stateful packet inspection.
Step 22	**end** **Example:** `Device(config-pmap-c)# end`	Exits QoS policy-map class configuration mode and enters privileged EXEC mode.

Configuring the Aggressive Aging of Firewall Sessions

You can configure the Aggressive Aging feature for per-box (per-box refers to the entire firewall session table), default-VRF, and per-VRF firewall sessions. Before the Aggressive Aging feature can work, you must configure the aggressive aging and the aging-out time of firewall sessions.

Perform the following tasks to configure the aggressive aging of firewall sessions.

Configuring per-Box Aggressive Aging

Per-box refers to the entire firewall session table. Any configuration that follows the **parameter-map type inspect-global** command applies to the box.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. Enter one of the following commands:
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats global**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	Enter one of the following commands:
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	Example:
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		Configures a global parameter map for connecting thresholds and timeouts and enters parameter-map type inspect configuration mode.
		• Based on your release, the **parameter-map type inspect-global** and the **parameter-map type inspect global** commands are supported. You cannot configure both these commands together.
		• Skip Steps 4 and 5 if you configure the **parameter-map type inspect-global** command.
		Note
		If you configure the **parameter-map type inspect-global** command, **per-box** configurations are not supported because, by default, all **per-box** configurations apply to all firewall sessions.

Step 4	**per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value*	**percent** *percent* **low percent** *percent*}	Configures the maximum limit and the aggressive aging rate for half-opened sessions in the firewall session table.

	Command or Action	Purpose
	Example: `Device(config-profile)# per-box max-incomplete 2000 aggressive-aging high 1500 low 1200`	
Step 5	**per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} **Example:** `Device(config-profile)# per-box aggressive-aging high 1700 low 1300`	Configures the aggressive aging limit of total sessions.
Step 6	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 7	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect pmap1`	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action and enters parameter-map type inspect configuration mode.
Step 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] **Example:** `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session. • After aggressive aging is enabled, the SYN wait timer of the oldest TCP connections are reset from the default to the configured ageout time. In this example, instead of waiting for 30 seconds for connections to timeout, the timeout of the oldest TCP connections are set to 10 seconds. Aggressive aging is disabled when the connections drop below the low watermark.
Step 9	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and enters privileged EXEC mode.
Step 10	**show policy-firewall stats global** **Example:** `Device# show policy-firewall stats global`	Displays global firewall statistics information.

Configuring Aggressive Aging for a Default VRF

When you configure the **max-incomplete aggressive-aging** `command, it applies to the default VRF.`

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enters one of the following commands:

- **parameter-map type inspect-global**
- **parameter-map type inspect global**

4. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}]
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats vrf global**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	Enters one of the following commands:
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	Example:
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		Configures a global parameter map for connecting thresholds and timeouts and enters parameter-map type inspect configuration mode.
		• Based on your release, the **parameter-map type inspect-global** and the **parameter-map type inspect global** commands are supported. You cannot configure both these commands together.
		• Skip Step 5 if you configure the **parameter-map type inspect-global** command.
		Note
		If you configure the **parameter-map type inspect-global** command, **per-box** configurations are not supported because, by default, all **per-box** configurations apply to all firewall sessions.

Step 4	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value*	**percent** *percent* **low percent** *percent*} **Example:**	Configures the maximum limit and the aggressive aging limit of half-opened firewall sessions.

	Command or Action	Purpose
	`Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255`	
Step 5	**session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}] **Example:** `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	Configures the total limit and the aggressive aging limit for total firewall sessions.
Step 6	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 7	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect pmap1`	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action and enters parameter-map type inspect configuration mode.
Step 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] **Example:** `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session. • After aggressive aging is enabled, the SYN wait timer of the oldest TCP connections are reset from the default to the configured ageout time. In this example, instead of waiting for 30 seconds for connections to timeout, the timeout of the oldest TCP connections are set to 10 seconds. Aggressive aging is disabled when the connections drop below the low watermark.
Step 9	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and enters privileged EXEC mode.
Step 10	**show policy-firewall stats vrf global** **Example:** `Device# show policy-firewall stats vrf global`	Displays global VRF firewall policy statistics.

Configuring per-VRF Aggressive Aging

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*

7. **exit**
8. **parameter-map type inspect-vrf** *vrf-pmap-name*
9. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
10. **session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}]
11. **alert on**
12. **exit**
13. Enter one of the following commands:
    - **parameter-map type inspect-global**
    - **parameter-map type inspect global**
14. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
15. **exit**
16. **parameter-map type inspect** *parameter-map-name*
17. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
18. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect match-any** *class-map-name*
22. **inspect** *parameter-map-name*
23. **end**
24. **show policy-firewall stats vrf** *vrf-pmap-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Device(config)# ip vrf ddos-vrf1`	Defines a VRF instance and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 100:2`	Specifies a route distinguisher (RD) for a VRF instance.

	Command or Action	Purpose
Step 5	**route-target export** *route-target-ext-community* **Example:** `Device(config-vrf)# route-target export 100:2`	Creates a route-target extended community and exports the routing information to the target VPN extended community.
Step 6	**route-target import** *route-target-ext-community* **Example:** `Device(config-vrf)# route-target import 100:2`	Creates a route-target extended community and imports routing information from the target VPN extended community.
Step 7	**exit** **Example:** `Device(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 8	**parameter-map type inspect-vrf** *vrf-pmap-name* **Example:** `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	Configures an inspect VRF-type parameter map and enters parameter-map type inspect configuration mode.
Step 9	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} **Example:** `Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200`	Configures the maximum limit and the aggressive aging limit for half-opened sessions.
Step 10	**session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}] **Example:** `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	Configures the total session limit and the aggressive aging limit for the total sessions. • You can configure the total session limit as an absolute value or as a percentage.
Step 11	**alert on** **Example:** `Device(config-profile)# alert on`	Enables the console display of stateful packet inspection alert messages.
Step 12	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.

Step 13	Enter one of the following commands:
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	Example:
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		Configures a global parameter map and enters parameter-map type inspect configuration mode.
		• Based on your release, the **parameter-map type inspect-global** and the **parameter-map type inspect global** commands are supported. You cannot configure both these commands together.
		• Skip Step 14 if you configure the **parameter-map type inspect-global** command.

	Command or Action	Purpose
		Note If you configure the **parameter-map type inspect-global** command, **per-box** configurations are not supported because, by default, all **per-box** configurations apply to all firewall sessions.
Step 14	**vrf** *vrf-name* **inspect** *vrf-pmap-name* **Example:** `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	Binds a VRF with a parameter map.
Step 15	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 16	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect pmap1`	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action and enters parameter-map type inspect configuration mode.
Step 17	**tcp idle-time** *seconds* [**ageout-time** *seconds*] **Example:** `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	Configures the timeout for idle TCP sessions and the aggressive aging-out time for TCP sessions.
Step 18	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] **Example:** `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session. • When aggressive aging is enabled, the SYN wait timer of the oldest TCP connections are reset from the default to the configured ageout time. In this example, instead of waiting for 30 seconds for connections to timeout, the timeout of the oldest TCP connections are set to 10 seconds. Aggressive aging is disabled when the connections drop below the low watermark.
Step 19	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 20	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect ddos-fw`	Creates a protocol-specific inspect type policy map and enters QoS policy-map configuration mode.
Step 21	**class type inspect match-any** *class-map-name* **Example:** `Device(config-pmap)# class type inspect match-any ddos-class`	Specifies the traffic (class) on which an action is to be performed and enters QoS policy-map class configuration mode.

	Command or Action	Purpose
Step 22	**inspect** *parameter-map-name* **Example:** `Device(config-pmap-c)# inspect pmap1`	Enables stateful packet inspection for the parameter map.
Step 23	**end** **Example:** `Device(config-pmap-c)# end`	Exits QoS policy-map class configuration mode and enters privileged EXEC mode.
Step 24	**show policy-firewall stats vrf** *vrf-pmap-name* **Example:** `Device# show policy-firewall stats vrf vrf1-pmap`	Displays VRF-level policy firewall statistics.

Example

The following is sample output from the **show policy-firewall stats vrf vrf1-pmap** command:

```
Device# show policy-firewall stats vrf vrf1-pmap

VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 80, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 116
       Half Open Aggressive Aging Period Off, Event Count: 0
```

Configuring the Aging Out of Firewall Sessions

You can configure the aging out of ICMP, TCP, or UDP firewall sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
5. **exit**
6. **parameter-map type inspect** *parameter-map-name*

7. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **exit**
10. **policy-map type inspect** *policy-map-name*
11. **class type inspect match-any** *class-map-name*
12. **inspect** *parameter-map-name*
13. **end**
14. **show policy-firewall stats vrf** *vrf-pmap-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	Enter one of the following commands:
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	Example:
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspectglobal`
		Configures a global parameter map and enters parameter-map type inspect configuration mode.
		• Based on your release, the **parameter-map type inspect-global** and the **parameter-map type inspect global** commands are supported. You cannot configure both these commands together.
		• Skip Step 4 if you configure the **parameter-map type inspect-global** command.
		Note
		If you configure the **parameter-map type inspect-global** command, **per-box** configurations are not supported because, by default, all **per-box** configurations apply to all firewall sessions.

Step 4	**vrf** *vrf-name* **inspect** *vrf-pmap-name* **Example:** `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	Binds a VRF with a parameter map.
Step 5	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 6	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect pmap1`	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action and enters parameter-map type inspect configuration mode.
Step 7	**tcp idle-time** *seconds* [**ageout-time** *seconds*] **Example:** `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	Configures the timeout for idle TCP sessions and the aggressive aging-out time for TCP sessions. • You can also configure the **tcp finwait-time** command to specify how long a TCP session will be managed after the firewall detects a finish (FIN) exchange, or you can configure the **tcp synwait-time** command to specify how long the software will wait for a TCP session to reach the established state before dropping the session.
Step 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] **Example:** `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session. • When aggressive aging is enabled, the SYN wait timer of the oldest TCP connections are reset from the default to the configured ageout time. In this example, instead of waiting for 30 seconds for connections to timeout, the timeout of the oldest TCP connections are set to 10 seconds. Aggressive aging is enabled when the connections drop below the low watermark.
Step 9	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 10	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect ddos-fw`	Creates a protocol-specific inspect type policy map and enters QoS policy-map configuration mode.
Step 11	**class type inspect match-any** *class-map-name* **Example:** `Device(config-pmap)# class type inspect match-any ddos-class`	Specifies the traffic class on which an action is to be performed and enters QoS policy-map class configuration mode.
Step 12	**inspect** *parameter-map-name* **Example:** `Device(config-pmap-c)# inspect pmap1`	Enables stateful packet inspection for the parameter map.
Step 13	**end** **Example:** `Device(config-pmap-c)# end`	Exits QoS policy-map class configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 14	**show policy-firewall stats vrf** *vrf-pmap-name* **Example:** `Device# show policy-firewall stats vrf vrf1-pmap`	Displays VRF-level policy firewall statistics.

Example

The following is sample output from the **show policy-firewall stats vrf vrf1-pmap** command:

```
Device# show policy-firewall stats vrf vrf1-pmap

 VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 270, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 12
       Half Open Aggressive Aging Period Off, Event Count: 0
```

Configuring Firewall Event Rate Monitoring

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **alert on**
5. **threat-detection basic-threat**
6. **threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
7. **threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
8. **threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
9. **exit**
10. **zone security** *security-zone-name*
11. **protection** *parameter-map-name*
12. **exit**
13. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
14. **end**
15. **show policy-firewall stats zone**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect-zone** *zone-pmap-name* **Example:** `Device(config)# parameter-map type inspect-zone zone-pmap1`	Configures an inspect-zone parameter map and enters parameter-map type inspect configuration mode.
Step 4	**alert on** **Example:** `Device(config-profile)# alert on`	Enables the console display of stateful packet inspection alert messages for a zone. • You can use the **log** command to configure the logging of alerts either to the syslog or to the high-speed logger (HSL).
Step 5	**threat-detection basic-threat** **Example:** `Device(config-profile)# threat-detection basic-threat`	Configures basic threat detection for a zone.
Step 6	**threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* **Example:** `Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	Configures the threat detection rate for firewall drop events. • You must configure the **threat-detection basic-threat** command before you configure the **threat-detection rate** command.
Step 7	**threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* **Example:** `Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	Configures the threat detection rate for firewall inspection-based drop events.
Step 8	**threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*	Configures the threat detection rate for TCP SYN attack events.

	Command or Action	Purpose
	Example: `Device(config-profile)# threat-detection rate syn-attack average-time-frame 600 average-threshold 100 burst-threshold 100`	
Step 9	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 10	**zone security** *security-zone-name* **Example:** `Device(config)# zone security public`	Creates a security zone and enters security zone configuration mode.
Step 11	**protection** *parameter-map-name* **Example:** `Device(config-sec-zone)# protection zone-pmap1`	Attaches the inspect-zone parameter map to the zone and applies the features configured in the inspect-zone parameter map to the zone.
Step 12	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and enters global configuration mode.
Step 13	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* **Example:** `Device(config)# zone-pair security private2public source private destination public`	Creates a zone pair and enters security zone-pair configuration mode.
Step 14	**end** **Example:** `Device(config-sec-zone-pair)# end`	Exits security zone-pair configuration mode and enters privileged EXEC mode.
Step 15	**show policy-firewall stats zone** **Example:** `Device# show policy-firewall stats zone`	Displays policy firewall statistics at the zone level.

Configuring the per-Box Half-Opened Session Limit

Per-box refers to the entire firewall session table. Any configuration that follows the **parameter-map type inspect-global** command applies to the box.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:

- **parameter-map type inspect-global**
- **parameter-map type inspect global**

4. **alert on**
5. **per-box max-incomplete** *number*
6. **session total** *number*
7. **end**
8. **show policy-firewall stats global**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	Enter one of the following commands:
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	Example:
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		Configures a global parameter map for connecting thresholds and timeouts and enters parameter-map type inspect configuration mode.
		• Based on your release, the **parameter-map type inspect-global** and the **parameter-map type inspect global** commands are supported. You cannot configure both these commands together.
		• Skip to Steps 5 and 6 if you configure the **parameter-map type inspect-global** command.
		Note
		If you configure the **parameter-map type inspect-global** command, **per-box** configurations are not supported because, by default, all **per-box** configurations apply to all firewall sessions.

Step 4	**alert on** **Example:** `Device(config-profile)# alert on`	Enables the console display of stateful packet inspection alert messages.
Step 5	**per-box max-incomplete** *number* **Example:** `Device(config-profile)# per-box max-incomplete 12345`	Configures the maximum number of half-opened connections for the firewall session table.

	Command or Action	Purpose
Step 6	**session total** *number* **Example:** `Device(config-profile)# session total 34500`	Configures the total session limit for the firewall session table.
Step 7	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and enters privileged EXEC mode.
Step 8	**show policy-firewall stats global** **Example:** `Device# show policy-firewall stats global`	Displays global firewall statistics information.

Configuring the Half-Opened Session Limit for an Inspect-VRF Parameter Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-name*
4. **alert on**
5. **max-incomplete** *number*
6. **session total** *number*
7. **exit**
8. Enter one of the following commands:
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
9. **alert on**
10. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
11. **end**
12. **show policy-firewall stats vrf** *vrf-pmap-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect-vrf** *vrf-name* **Example:** `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	Configures an inspect-VRF parameter map and enters parameter-map type inspect configuration mode.
Step 4	**alert on** **Example:** `Device(config-profile)# alert on`	Enables the console display of stateful packet inspection alert messages.
Step 5	**max-incomplete** *number* **Example:** `Device(config-profile)# max-incomplete 2000`	Configures the maximum number of half-opened connections per VRF.
Step 6	**session total** *number* **Example:** `Device(config-profile)# session total 34500`	Configures the total session limit for a VRF.
Step 7	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.

Step 8	Enter one of the following commands:
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	Example:
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		Configures a global parameter map for connecting thresholds and timeouts and enters parameter-map type inspect configuration mode.
		• Based on your release, you can use either the **parameter-map type inspect-global** command or the **parameter-map type inspect global** command. You cannot configure both these commands together.
		• Skip Step 10 if you configure the **parameter-map type inspect-global** command.
		Note
		If you configure the **parameter-map type inspect-global** command, **per-box** configurations are not supported because, by default, all **per-box** configurations apply to all firewall sessions.

Step 9	**alert on** **Example:** `Device(config-profile)# alert on`	Enables the console display of stateful packet inspection alert messages.

	Command or Action	Purpose
Step 10	**vrf** *vrf-name* **inspect** *vrf-pmap-name* **Example:** `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	Binds the VRF to the global parameter map.
Step 11	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and enters privileged EXEC mode.
Step 12	**show policy-firewall stats vrf** *vrf-pmap-name* **Example:** `Device# show policy-firewall stats vrf vrf1-pmap`	Displays VRF-level policy firewall statistics.

Configuring the Global TCP SYN Flood Limit

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box tcp syn-flood limit** *number*
6. **end**
7. **show policy-firewall stats vrf global**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **parameter-map type inspect-global**	Configures a global parameter map and enters parameter-map type inspect configuration mode.

	Command or Action	Purpose

	• **parameter-map type inspect global**
	Example:
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		• Based on your release, you can configure either the **parameter-map type inspect-global** command or the **parameter-map type inspect global** command. You cannot configure both these commands together.
		• Skip Step 5 if you configure the **parameter-map type inspect-global** command.
		Note
		If you configure the **parameter-map type inspect-global** command, **per-box** configurations are not supported because, by default, all **per-box** configurations apply to all firewall sessions.

Step 4	**alert on** **Example:** `Device(config-profile)# alert on`	Enables the console display of stateful packet inspection alert messages.
Step 5	**per-box tcp syn-flood limit** *number* **Example:** `Device(config-profile)# per-box tcp syn-flood limit 500`	Limits the number of TCP half-opened sessions that trigger SYN cookie processing for new SYN packets.
Step 6	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and enters privileged EXEC mode.
Step 7	**show policy-firewall stats vrf global** **Example:** `Device# show policy-firewall stats vrf global`	(Optional) Displays the status of the global VRF firewall policy. • The command output also displays how many TCP half-opened sessions are present.

Example

The following is sample output from the **show policy-firewall stats vrf global** command:

```
Device# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

Configuring Firewall Resource Management

Note A global parameter map takes effect on the global routing domain and not at the router level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **session total** *number*
5. **tcp syn-flood limit** *number*
6. **exit**
7. **parameter-map type inspect-global**
8. **vrf** *vrf-name* **inspect** *parameter-map-name*
9. **exit**
10. **parameter-map type inspect-vrf vrf-default**
11. **session total** *number*
12. **tcp syn-flood limit** *number*
13. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect-vrf** *vrf-pmap-name* **Example:** `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	Configures an inspect VRF-type parameter map and enters parameter-map type inspect configuration mode.
Step 4	**session total** *number* **Example:** `Device(config-profile)# session total 1000`	Configures the total number of sessions.

	Command or Action	Purpose
Step 5	**tcp syn-flood limit** *number* **Example:** `Device(config-profile)# tcp syn-flood limit 2000`	Limits the number of TCP half-opened sessions that trigger synchronization (SYN) cookie processing for new SYN packets.
Step 6	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 7	**parameter-map type inspect-global** **Example:** `Device(config)# parameter-map type inspect-global`	Configures a global parameter map and enters parameter-map type inspect configuration mode.
Step 8	**vrf** *vrf-name* **inspect** *parameter-map-name* **Example:** `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	Binds a VRF to the parameter map.
Step 9	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 10	**parameter-map type inspect-vrf vrf-default** **Example:** `Device(config)# parameter-map type inspect-vrf vrf-default`	Configures a default inspect VRF-type parameter map.
Step 11	**session total** *number* **Example:** `Device(config-profile)# session total 6000`	Configures the total number of sessions. • You can configure the **session total** command for an inspect VRF-type parameter map and for a global parameter map. When you configure the **session total** command for an inspect VRF-type parameter map, the sessions are associated with an inspect VRF-type parameter map. The **session total** command is applied to the global routing domain when it is configured for a global parameter-map.
Step 12	**tcp syn-flood limit** *number* **Example:** `Device(config-profile)# tcp syn-flood limit 7000`	Limits the number of TCP half-opened sessions that trigger SYN cookie processing for new SYN packets.
Step 13	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and enters privileged EXEC mode.

Configuration Examples for IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management

Example: Configuring an IPv6 Firewall

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

Example: Configuring the Aggressive Aging of Firewall Sessions

Example: Configuring per-Box Aggressive Aging

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# per-box max-incomplete 2000 aggressive-aging 1500 low 1200
Device(config-profile)# per-box aggressive-aging high 1700 low 1300
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

Example: Configuring Aggressive Aging for a Default VRF

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60
Device(config-profile)# exit
```

```
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

Example: Configuring per-VRF Aggressive Aging

```
Device# configure terminal
Device(config)# ip vrf ddos-vrf1
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# exit
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60
Device(config-profile)# alert on
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-pmap)# class type inspect match-any ddos-class
Device(config-pmap-c)# inspect pmap1
Device(config-profile)# end
```

Example: Configuring the Aging Out of Firewall Sessions

```
Device# configure terminal
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-profile)# class type inspect match-any ddos-class
Device(config-profile)# inspect pmap1
Device(config-profile)# end
```

Example: Configuring Firewall Event Rate Monitoring

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect zone zone-pmap1
Device(config-profile)# alert on
Device(config-profile)# threat-detection basic-threat
Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold
 100 burst-threshold 100
Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600
```

```
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate syn-attack average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# exit
Device(config)# zone security public
Device(config-sec-zone)# protection zone-pmap1
Device(config-sec-zone)# exit
Device(config)# zone-pair security private2public source private destination public
Device(config-sec-zone-pair)# end
```

Example: Configuring the per-Box Half-Opened Session Limit

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box max-incomplete 12345
Device(config-profile)# session total 34500
Device(config-profile)# end
```

Example: Configuring the Half-Opened Session Limit for an Inspect VRF Parameter Map

```
Device# configure terminal
Device(config)# parameter-map type inspect vrf vrf1-pmap
Device(config-profile)# alert on
Device(config-profile)# max-incomplete 3500
Device(config-profile)# session total 34500
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# end
```

Example: Configuring the Global TCP SYN Flood Limit

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box tcp syn-flood limit 500
Device(config-profile)# end
```

Example: Configuring Firewall Resource Management

```
Device# configure terminal
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# session total 1000
Device(config-profile)# tcp syn-flood limit 2000
```

```
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# vrf vrf1 inspect pmap1
Device(config-profile)# exit
Device(config)# parameter-map type inspect-vrf vrf-default
Device(config-profile)# session total 6000
Device(config-profile)# tcp syn-flood limit 7000
Device(config-profile)# end
```

Additional References for IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management

Feature Name	Releases	Feature Information
IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management	Cisco IOS XE Release 3.7S	IPv6 zone-based firewalls support the Protection of Distributed Denial of Service Attacks and the Firewall Resource Management features. The Protection Against Distributed Denial of Service Attacks feature provides protection from Denial of Service (DoS) attacks at the global level (for all firewall sessions) and at the VPN routing and forwarding (VRF) level. You can configure the aggressive aging of firewall sessions, event rate monitoring of firewall sessions, half-opened connections limit, and global TCP SYN cookie protection to prevent distributed DoS attacks. The Firewall Resource Management feature limits the number of VPN routing and forwarding (VRF) instances and global firewall sessions that are configured on a device.
IPv6 Firewall Support for Prevention of Distributed Denial of Service Attacks and Resource Management	Cisco IOS XE Release 3.10S	In Cisco IOS XE Release 3.10S, support was added for Cisco CSR 1000V Series Routers.